

Livre blanc

Modernisez votre cybersécurité dès maintenant : 10 raisons de le faire et 10 façons de le faire

16 septembre 2021





À propos de l'auteur

Rob Krug, Responsable/en charge de l'architecture de sécurité, Avast Business

Rob travaille dans le domaine de l'ingénierie et de la sécurité des réseaux depuis plus de 30 ans. Il a notamment travaillé dans le domaine des télécommunications, de la conception et de la gestion de réseaux et, surtout, de la sécurité des réseaux.

Spécialisé dans les vulnérabilités de sécurité, Rob a une expérience étendue de la cryptographie, du piratage éthique et de l'ingénierie inverse des logiciels malveillants. Rob a servi dans la marine américaine et a également travaillé en tant qu'analyste de la sécurité des données et directeur de l'ingénierie pour plusieurs fournisseurs de services et vendeurs internationaux. Rob a conçu, mis en œuvre et maintenu certains des réseaux les plus complexes et les plus sécurisés que l'on puisse imaginer.

Soyons réalistes. Votre organisation ne fait probablement pas tout ce qu'elle pourrait faire pour assurer la sécurité de ses utilisateurs et de ses ressources informatiques. Vous êtes au courant des piratages les plus médiatisés et des vulnérabilités exploitées, et naturellement, cela vous inquiète. Mais la sécurité n'est pas la seule chose qui absorbe les ressources limitées de votre organisation, et d'ailleurs, vous n'avez pas subi de violation grave. Jusqu'à présent, en tout cas.

Comme d'autres entreprises l'ont appris à leurs dépens, l'espoir est un trait humain précieux, mais ce n'est pas une base solide pour une stratégie de sécurité. Heureusement, il existe des raisons impérieuses de se concentrer sur l'amélioration de la sécurité de votre entreprise et des mesures que vous pouvez prendre dès aujourd'hui pour y parvenir de manière significative.

10 raisons de moderniser votre cybersécurité maintenant

1 Réduire les risques

Une sécurité plus efficace, multicouche et omniprésente assure une meilleure protection de vos utilisateurs et de vos ressources informatiques. Cela réduit les risques multiples, comme le risque d'être victime d'une brèche de sécurité ou d'échouer à un audit.

2 Minimiser les coûts informatiques et de sécurité

L'étude 2015 sur le coût des brèches de données, menée par Ponemon Institute et sponsorisée par IBM, a interrogé plus de 1 500 praticiens de l'informatique, de la conformité et de la sécurité de l'information dans 350 organisations de 11 pays. L'étude a révélé que le coût total consolidé moyen d'une brèche de données est de 3,8 millions de dollars, soit une augmentation de 23 % depuis 2013. En outre, le coût encouru pour chaque perte ou volé contenant des informations sensibles et confidentielles a augmenté de six pour cent, passant d'une moyenne consolidée de 145 à 154 dollars. L'amélioration de la sécurité réduit également le temps et l'argent nécessaires pour remédier aux vulnérabilités exploitées avec succès, et permet une meilleure et plus fréquente automatisation de la réduction des coûts.

3 Protéger en silence

Une sécurité moderne et réellement efficace est omniprésente, ubiquitaire et invisible, et n'a que peu ou pas d'impact sur la productivité des utilisateurs ou les activités de l'entreprise. La capacité d'améliorer la sécurité sans perturbation est essentielle à la satisfaction des utilisateurs et à l'adoption généralisée de nouvelles fonctionnalités et de nouveaux outils.



4 Voir plus, savoir plus et protéger plus

Une protection maximale exige une visibilité et une connaissance maximales de votre environnement informatique et de sa posture de sécurité. Seuls des outils modernes et intégrés peuvent offrir cette visibilité et vous permettre d'assurer la meilleure sécurité possible dans votre environnement et votre organisation.

5 Renforcer l'agilité

Votre organisation doit devenir et rester agile pour survivre et prospérer face à la concurrence. En d'autres termes, il n'y a pas d'agilité sans une sécurité complète et cohérente.

6 Augmenter la résilience de l'entreprise

Une étude réalisée en 2013 par Ponemon Institute et sponsorisée par Emerson Network Power a révélé que les temps d'arrêt des centres de données coûtent environ 7 900 dollars par minute. Une étude de 2014 menée par Avaya a révélé que chaque incident de temps d'arrêt coûte entre 140 000 et 540 000 dollars, en fonction de la taille et du type d'entreprise concernée. Et un sondage réalisé en 2015 par Kaspersky Lab et B2B International a révélé qu'il peut coûter de 38 000 à 551 000 dollars pour se remettre d'une seule violation de la cybersécurité. Des statistiques telles que celles-ci renforcent la résilience - c'est-à-dire la capacité de votre entreprise à minimiser les temps d'arrêt planifiés et non planifiés - une nécessité absolue.

7 Développer la crédibilité

Edelman, la plus grande société de relations publiques au monde, a sondé près de 33 000 personnes pour son baromètre de la confiance 2015. Environ 63 % des personnes interrogées ont déclaré qu'elles préféraient tout simplement ne pas faire affaire avec ceux en qui elles n'ont pas confiance, tandis que 80 % ont déclaré qu'elles ne faisaient affaire qu'avec des personnes et des entreprises fiables. Et sans une sécurité moderne et efficace, il est difficile, voire impossible, d'assurer et de démontrer la fiabilité de la confiance.

8 Favoriser une sécurité centrée sur l'utilisateur

L'informatique moderne, centrée sur l'utilisateur, se concentre moins sur les appareils, les fichiers et les outils que sur l'expérience de l'utilisateur. Pour mettre en place une informatique centrée sur l'utilisateur, votre entreprise a besoin d'une sécurité centrée sur l'utilisateur - une protection multicouche et intégrée de tous les utilisateurs, ressources, connexions et dispositifs autorisés.

Emerson Network Power a constaté que les temps d'arrêt des centres de données coûtent **environ 7 900 $ par minute**. Une étude menée en 2014 par Avaya a révélé que chaque incident de **temps d'arrêt coûte entre 140 000 et 540 000 $**, en fonction de la taille et du type d'entreprise affectée.



9 **Opérationnaliser la sécurité**

La gestion moderne de la sécurité est moins réactive et tactique, et plus axée sur les opérations et proactive. Dans les grandes organisations, le personnel opérationnel assume de plus en plus de fonctions liées à la sécurité, ce qui permet aux spécialistes de la sécurité de se concentrer davantage sur des questions plus complexes et stratégiques. Pour les petites et moyennes entreprises, la tendance est de délaisser les mesures réactives et de s'orienter vers la mise en œuvre continue de mesures de sécurité nouvelles et optimisées et vers des opérations de sécurité (ou "SecOps") plus efficaces et proactives).

10 **Être prêt pour l'avenir**

Selon le rapport Verizon 2015 sur les enquêtes relatives aux violations de données, il y a dix ans, quelque 70 % de l'activité des logiciels malveillants était imputable à seulement sept familles ou types de logiciels malveillants. En 2014, ces 70 % de l'activité des logiciels malveillants étaient répartis entre 20 types de logiciels malveillants différents. Au cours de cette même période, les logiciels malveillants ont considérablement évolué, passant de "vers" de messageries électroniques à "l'adhésion furtive à un botnet de commande et de contrôle, au vol d'informations d'identification et à une certaine forme de fraude" Cette même étude estime que cinq événements liés aux logiciels malveillants se produisent chaque seconde de chaque jour. Seule une sécurité moderne, stratifiée et centrée sur l'utilisateur peut offrir la protection et l'adaptabilité dont votre entreprise a besoin aujourd'hui et aura besoin demain.



10 façons de moderniser votre cybersécurité maintenant

Mettez en place des correctifs complets et en temps opportun sur l'ensemble de vos systèmes critiques :

1 **Systèmes d'exploitation**

2 **Applications tierces**

- et -

3 **Les appareils de votre réseau, qu'ils soient locaux, distants ou mobiles**



4 Établir une liste blanche d'applications (et une liste noire, le cas échéant) non-intrusive et non perturbatrice

Si vous ne faites rien de plus que les quatre étapes ci-dessus, vous pouvez faire de grands progrès pour améliorer la sécurité et la protection de votre organisation.

5 Automatisez autant que possible vos processus éprouvés de gestion des correctifs et de la sécurité

Cela permettra d'optimiser la cohérence de l'exécution et l'évolutivité de ces processus.

6 Intégrez la gestion proactive des correctifs dans et avec toutes les autres initiatives informatiques importantes de votre organisation, en particulier celles axées sur la gestion des actifs informatiques (ITAM), la gestion des opérations informatiques (ITOM) ou la gestion des services informatiques (ITSM)

Une sécurité multicouche, efficace et centrée sur l'utilisateur est essentielle au succès de ces efforts.

7 Engagez, éduquez et motivez les utilisateurs pour qu'ils comprennent l'importance d'une sécurité efficace

Vos utilisateurs sont vos premières et dernières lignes de défense. Une sécurité complète, efficace et centrée sur l'utilisateur vise à les protéger pour qu'ils ne soient pas victimes de malfaiteurs et qu'ils ne soient pas les vecteurs d'actes répréhensibles. Elle encourage également les utilisateurs (y compris les clients) à signaler les incidents et les comportements suspects au support informatique, à la sécurité, ou aux deux, dès que possible.

8 Ne pas faire cavalier seul

Les entreprises décident de plus en plus souvent que l'importance et la demande croissante d'une sécurité informatique efficace sont trop grandes pour être laissées entre les mains des seules équipes informatiques et de sécurité. Un grand nombre d'entre elles séparent également les budgets et les activités de sécurité de l'informatique classique et répartissent ces budgets, ces efforts et cette sensibilisation sur l'ensemble de l'organisation. Certaines entreprises bien connues et très respectées sont réputées pour leur "crowdsourcing" d'informations et de renseignements sur la sécurité. Vous pouvez commencer par impliquer des collègues d'autres départements de votre propre organisation.

Selon l'Australian Signals Directorate, **jusqu'à 85 % des attaques ciblées** peuvent être évitées en établissant une liste blanche, en appliquant des correctifs aux systèmes d'exploitation et aux applications tierces et en limitant les privilèges administratifs

Selon la base de données nationale américaine sur les vulnérabilités, **86 % des vulnérabilités signalées** proviennent d'applications tierces.

Selon le rapport d'enquête sur les violations de données 2015 (Data Breach Investigations Report) de Verizon, **99,9 % des vulnérabilités exploitées** en 2014 ont été compromises plus d'un an après la publication de la vulnérabilité.

Un sondage Ponemon Institute/IBM mené auprès d'environ 200 clients ayant fait l'objet d'une brèche a révélé que seulement **45 % de ces brèches** étaient causées par des activités ou des logiciels malveillants. Les **55 % restants ont été causés par des erreurs opérationnelles**, des erreurs involontaires d'utilisateurs légitimes ou des problèmes de systèmes.



9 **Utilisez les renseignements sur votre environnement et les rapports personnalisés pour identifier et hiérarchiser les menaces, pour promouvoir et encourager le soutien aux initiatives de sécurité, et pour guider et soutenir les décisions liées à la sécurité**

Les renseignements sur l'infrastructure et les rapports basés sur des données "réelles" de votre propre environnement peuvent souvent être les outils de communication les plus convaincants et les plus efficaces avec vos collègues au sein et au-delà de vos équipes informatiques et de sécurité.

10 **S'efforcer de faire de la formation continue en tant qu'évolution de la sécurité dans votre entreprise une priorité pour tout le monde**

Comme l'a déclaré Lawrence Pingree, analyste chez Gartner, au New York Times en octobre 2015, "Il existe 600 millions de fichiers individuels connus pour être bons, et un univers de logiciels malveillants d'environ 400 millions de fichiers. Mais il y a aussi 100 millions de logiciels publicitaires potentiellement indésirables, et 200 millions de logiciels qui ne sont tout simplement pas connus. Il faut beaucoup de talent pour déterminer ce qui est normal et ce qui ne l'est pas."

Vous n'avez aucun moyen de savoir si l'un de ces 400 millions de logiciels malveillants connus est susceptible de cibler votre entreprise ou quand cela se produira - si ce n'est déjà fait. Et bien que les entreprises dépensent quelque 30 milliards de dollars par an en outils de sécurité, les vulnérabilités et les menaces se transforment chaque jour en véritables brèches. En modernisant vos outils et processus de sécurité informatique, vous et votre équipe pouvez améliorer sensiblement la sécurité de manière à étendre les protections actuelles et à vous préparer efficacement à l'avenir, quel qu'il soit.

Avast Business - Une cybersécurité tout-en-un pour le lieu de travail moderne



Avast Business offre une protection multicouche pour protéger vos utilisateurs et vos ressources informatiques contre les menaces les plus sophistiquées. Les solutions comprennent un antivirus de nouvelle génération, le test, le déploiement et la gestion automatisés des correctifs pour les systèmes Microsoft Windows et les applications tierces, la sauvegarde dans le cloud, les passerelles web sécurisées, l'accès réseau de confiance zéro (ZTN), etc.

Nos solutions sont intégrées dans une plateforme de sécurité unique. Cela permet une automatisation rapide des politiques de sécurité et de gestion informatique, et offre une visibilité inégalée sur les activités de sécurité et de gestion informatique.

La plateforme de sécurité d'Avast Business propose également des rapports et des tableaux de bord complets et configurables. Ceux-ci permettent d'améliorer la visibilité des risques et des menaces, de faciliter la conformité aux réglementations et aux politiques, et d'améliorer votre posture de sécurité globale. Pour plus d'informations, contactez votre responsable de compte Avast Business ou visitez www.avast.com/business.